REMARKS

Claims 1, 10, and 26-28 are pending.
Claims 1 and 26-28 are rejected.
Claim 10 is objected to.

The claimed inventions offer solutions to the following problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. The documents made of record, alone and in the aggregate, do not teach or suggest a solution to this problem.

The office action dated May 25, 2005 indicates that claims 27-28 are rejected under 35 USC §103(a) as being obvious over Hung et al. U.S. Patent No. 5,343,525 in view of Sako Patent No. JP9045008. This rejection is respectfully traversed because neither document teaches or suggests performing a bitwise XOR of an encryption mask and a block of ECC-encoded data.

Hung et al. disclose a system in which data is encrypted and decrypted by inverting it (col. 2, lines 46-48). Hung et al.'s enciphering/deciphering circuit 1 includes XOR gates X1 and X2. Each gate X1 has two inputs: a first input connected to VCC and a second input connected to a data bit line (col. 2, lines 42-45). A switch SW1 selects an encrypting path or a non-encrypting path (col. 3, lines 22-23). Bit inversion is performed in the encrypting path (col. 2, lines 46-48).

Moreover, Hung et al. are silent about when and where ECC-encoding and decoding are performed. If Hung et al.'s hard disk performs ECC-encoding and ECC-decoding, then the inversion-based encryption is not performed on ECC blocks.

PAGE 5/10 * RCVD AT 7/22/2005 1:03:35 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-46

The office action states that Sako's Abstract teaches that an ECC block can be encrypted. It does not. Here is the entirety of Sako's Abstract:

> PROBLEM TO BE SOLVED: To encrypt data in a simple constitution and access at high speed. SOLUTION: In an error-correcting code format, a sector 73 is constituted of a head part 71 and a user data part 72. An error correction C1 direction is set in a R/W direction and a C1 parity 74 is generated and added. On the other hand, an error correction C2 direction is set in a direction oblique to the C1 direction and a C2 parity 75 is generated and added. Data excluding at least the head part 71, e.g., a part 76 in the same row as the head pat 71 among the data handled in an error-correcting code process are converted in accordance with an encryption flag data.

Sako's abstract is concerned with error code correction, not encryption (Sako's parity is used in the context of error correction[1]). The last sentence of Sako's Abstract is vague and unclear. It is not clear whether ECC-encoded data is excluded from conversion, whether conversion is performed before or after ECC encoding, or whether conversion actually means encryption. Thus, Sako's Abstract alone provides no basis to assume that encryption is performed on ECC-encoded data.

Regardless, Sako's Abstract does not specify a type of encryption. The Abstract does not provide a reason, incentive or motivation to perform **XOR** encryption of an ECC-encoded block. Therefore, claims 27-28 should be allowed over the combination of Hung et al. and Sako.

The office action indicates that claim 28 is further rejected under 35 USC §103(a) as being obvious Schneier (Applied Cryptography, 2nd ed., 1996)

1 See the attached article entitled "Writing Quality." According to the article, C1 and C2 are Reed-Solomon Codes.

PAGE 6/10 * RCVD AT 7/22/2005 1:03:35 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-46

in view of Sako. Neither document provides reason, incentive or motivation for performing XOR encryption on ECC blocks. Moreover, Sako does not clearly teach encryption on ECC blocks. Therefore, the '103 rejection of claim 28 should be withdrawn.

The examiner gives reasons for combining the teachings of Schneier and Sako (ease of implementation and encryption speed). However, these reasons do not come from the prior art. The examiner does not cite a document providing those reasons. The examiner provides no analysis of the ease and speed relative to other types of encryption. The examiner ignores drawbacks of XOR encryption (that is, reasons against using XOR encryption), such as the relative ease of breaking it. Moreover, the examiner provides no evidence in the prior art of encrypting of ECC blocks. The examiner only provides an unsubstantiated allegation. Pursuant to MPEP §707 and 37 CFR §1.104(d)(2), the examiner is respectfully requested to cite a document or provide an affidavit that sets forth a reason, incentive or motivation for using XOR encryption on ECC blocks.

Claims 1 and 26 are rejected under the judicially-created doctrine of double-patenting. However, the office action provides no analysis of the prior art, and provides no indication as to whether claims 1 and 26 contain allowable subject matter. MPEP 706.03 states "The primary object of the examination of an application is to determine whether or not the claims are patentable over the prior art. This consideration should not be relegated to a secondary position while undue emphasis is given to nonprior art or 'technical' rejections." According to MPEP 706.03, double-patenting and nonstatutory subject matter are considered nonprior art rejections. The examiner is respectfully requested to indicate whether claims 1 and 26 contain allowable over the documents made of record.

PAGE 7/10 * RCVD AT 7/22/2005 1:03:35 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-46

It is respectfully submitted that the present application is in condition for allowance. The examiner is encouraged to contact the undersigned to discuss any remaining issues.

PAGE 8/10 * RCVD AT 7/22/2005 1:03:35 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:949 454 0898 * DURATION (mm-ss):04-46